

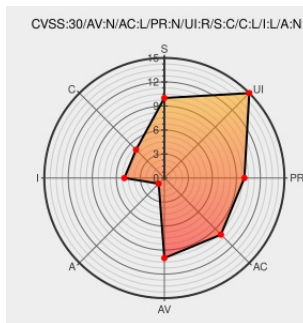


CVE-2018-10571

Published on: 04/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10571

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openemr](#) from [Open-emr](#) contain the following vulnerability:

Multiple reflected cross-site scripting (XSS) vulnerabilities in OpenEMR before 5.0.1 allow remote attackers to inject arbitrary web script or HTML via the (1) patient parameter to interface/main/finder/finder_navigation.php; (2) key parameter to interface/billing/get_claim_file.php; (3) formid or (4) formseq parameter to interface/orders/types.php; (5) eraname, (6) payday, (7) post_to_date, (8) deposit_date, (9) debug, or (10) InsId parameter to interface/billing/sl_eob_process.php; (11) form_source, (12) form_paydate, (13) form_deposit_date, (14) form_amount, (15) form_name, (16) form_pid, (17) form_encounter, (18) form_date, or (19) form_to_date parameter to interface/billing/sl_eob_search.php; (20) codetype or (21) search_term parameter to interface/de_identification_forms/find_code_popup.php; (22) search_term parameter to interface/de_identification_forms/find_drug_popup.php; (23) search_term parameter to interface/de_identification_forms/find_immunization_popup.php; (24) id parameter to interface/forms/CAMOS/view.php; (25) id parameter to interface/forms/reviewofs/view.php; or (26) list_id parameter to library/custom_template/personalize.php.

CVE-2018-10571 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
security fixes (#1519) · openemr/openemr@699e3c2 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/openemr/openemr/commit/699e3c2ef68545357cac714505df1419b8
Security issues reported by outside group · Issue #1518 · openemr/openemr · GitHub	Third Party Advisory github.com text/html	 MISC github.com/openemr/openemr/issues/1518
Release Features - OpenEMR Project Wiki	Release Notes Third Party Advisory Vendor Advisory www.open-emr.org text/html	 MISC www.open-emr.org/wiki/index.php/Release_Features#Version_5.0.1
security fixes by bradymiller · Pull Request #1519 · openemr/openemr · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/openemr/openemr/pull/1519
OpenEMR 弱點分析 – 資安最前線	csticsfrontline.wordpress.com text/html	 MISC csticsfrontline.wordpress.com/2018/05/24/openemr-%E5%BC%B1%E9%BB%9E%E5%88%86%E6%9E%90/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open-emr	Openemr	All	All	All	All
Application	Open-emr	Openemr	All	All	All	All
cpe:2.3:a:open-emr:openemr:*****:						
cpe:2.3:a:open-emr:openemr:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)